Annual General Meeting
of ISACA Bangalore Chapter on 19-Oct-2019
SPONSORS FOR 22\textsuperscript{nd} ANNUAL KARNATAKA CONFERENCE - JULY 2019

Gold

Canara Bank

 SyndicateBank

Silver

ASSERTION\textsuperscript{®}

Bronze

Neridio

CYBERPWN

Partners

KPMG

Qualys

TGroup
From The Desk Of The President

Dear Friends,

Greetings.

As you all are aware, our 22nd Annual Karnataka Conference went on very well in Hotel “Vivanta by Taj” on 19th and 20th July 2019. The theme of the conference was “Cyber Resiliency in Digital Era”.

The Conference was well attended on both the days. Mr. A. S. Kiran Kumar, Member, SPACE Commission, Government of India was the Chief Guest; Mr. Atul Kumar, CIO Syndicate Bank was the Guest of Honour and Mr. Jose Varghese, Co-Founder, Paladion was the Key Note Speaker on Day 1. On Day 2, Mr. V. Jayaraman, GM Canara Bank was the Chief Guest, and Mr. Arun Khannur, noted Product and Process Quality Consultant was the Key note speaker.

The conference included a plethora of speakers from various sectors of industry presenting on a variety of topics. The feedback received from delegates of the conference was overwhelming.

The Conference was supported by a record number of sponsors viz., CANARA BANK, SYNDICATE BANK, ASSERTION, NERIDIO, CYBERPWN, KPMG, QUALYS & TGROUP.

I thank one and all who made the event a grand success.

During the current year (2018-19), we conducted several CPE sessions including a pre-conference COBIT workshop. Our members participated in all the programmes with great enthusiasm and our CPE product made a good jump. Also, successfully conducted 5 rounds of Intro-seminar and 4 training sessions for CISA and CISM, 3 sessions for CRISC and 1 session for CGEIT exam aspirants. More such sessions are planned in the coming months.

In terms of membership, our growth was remarkable during the year 2018-19 and the Chapter has a registered membership of 1315 members as on 31st August, 2019 (1192 as on 31st Aug 2018).

My sincere thanks to all the members and my colleagues in the Executive Committee for providing excellent support in all the Chapter related activities. Our team is signing off and the new Team will take over the reins.

Request all to attend the AGM to be held on 19-Oct-2019 without fail.

With warm regards,

SRIDHAR S.
President
Message From the Vice President

Dear Members,

Greetings!!

After a successful Annual Conference it is time for the Annual General Meeting.

We had a great 22nd Annual Conference with the theme ‘Cyber Resiliency in Digital Era’ on 19th and 20th July, 2019 at Hotel Vivanta by Taj. The conference was attended by more than 200 participants on both the days with a great line of speakers from the industry. The conference was very well received by all the participants with good feedback. I would like to thank all the speakers and attendees for active participation and special thanks to our sponsors Syndicate Bank, Canara Bank, assertion, NERIDIO, Cyberpwn, KPMG, Qualys & TGROUP for their continuous support and making this event a grand success.

With introduction of CBT - Computer Based Testing and continuous testing model by ISACA, where exams are available throughout the year, we continue conducting weekend review classes at the chapter office for all 4 certifications - CISA, CISM, CRISC & CGEIT for the exam aspirants helping them achieve their career aspirations. I would also like to thank all the faculties who have been actively supporting in facilitating these classes and imparting knowledge to the participants.

Also throughout the year 2018-19 we had several CPE sessions, special CPE sessions and web based CPE session using Zoom platform with lot of interesting topics, helping members gain CPE hours as well as knowledge. There is a lot of interest and enthusiasm shown by members attending the Web based CPE sessions which are convenient and you can join from anywhere. We continue to conduct more such sessions and need your support.

It is time for AGM and 2019-20 EC (Executive Committee) formation. The 23rd Annual General Meeting (AGM) is planned on 19th October, 2019 at Trinity Isle Hotel between 5:00 pm to 8:30 pm and requesting all eligible members to attend the same to understand the chapter activities in detail.

ISACA 2020 Membership, Certifications renewal with CPE hours submission and Chapter membership renewal is NOW OPEN - requesting all to renew the same at the earliest.

As always, we solicit your active participation in the chapter’s various events and initiatives including monthly CPE meetings, newsletter article contribution, Review Classes for aspiring students and more.

Looking forward to meeting you at the AGM !!

With warm Regards,

SATISH KUMAR DWIBHASHI, CISA, CISM, CRISC, CGEIT
Vice-President
Message From Secretary

Dear Members,

Greetings!!

We had an overwhelming response and participation in the 22nd Annual Karnataka Conference with the theme “Cyber Resiliency in Digital Era” which was on 19th & 20th of July 2019. We witnessed a power packed presentations by the stalwart speakers from the industry. We had the largest number of sponsors for the first ever time for the Annual Conference.

We are now heading towards the AGM (Annual General Meeting) where we will provide an update on the initiatives taken and activities conducted by us to the Members of Bangalore Chapter. You as members can get inputs and can provide suggestions on the way forward and also will get the opportunity to elect the new EC (Executive Committee) for the year 2019-2020.

This year was very engaging and eventful with loads of programs, initiatives, CPEs and Special CPEs that were conducted. Members were given opportunity to participate in all the programs and was very well leveraged by the members who participated in almost all of them. To name a few activities conducted:

- Intro-Seminar conducted 5 times in various locations including Corporate
- Successfully completed 4 training batches for CISA & CISM
- Successfully completed 3 training batches for CRISC
- Successfully completed 1 training batch for CGEIT

My sincere thanks to all the members and my colleagues in the Executive Committee for providing excellent support in all the Chapter related activities. Our team is signing off and the new Team will take over the reins. Request you all to attend the AGM without fail.

Looking forward to meeting you at the AGM!

Regards,

VELMURUGA VENKATESH, CRISC, COBIT-5(F), ISO 27001 LA, ISO 31000
Secretary
Chapter Highlights for the period from July to September 2019

Workshop:

- Topic: Workshop on Enhancing Cyber Resiliency of Digital Enterprises by using COBIT 2019
- Venue: Hotel Trinity Isle, 139, S. C. Road, Seshadripuram, Bangalore.
- Date: 06-July-2019, Time: 9:30 AM - 5:30 PM

A One Day Free Workshop was conducted for the first 100 Registrants for the 22nd Annual Conference. The workshop was designed and conducted by CA. A. Rafea, Past Member of COBIT 5 Task Force/Expert Reviewer of COBIT 2019.

CPE credits: 7 Hours of CPE credits awarded.

Total Participants: 74.

Program was very well appreciated by all participants.

22nd Annual Karnataka Conference
Held On 19th and 20th July 2019:

- Venue: Vivanta by Taj, 1, M. G. Road, Bangalore.

The 22nd Annual Conference was centered around the theme - “Cyber Resiliency In Digital Era” and was attended by 174 registered delegates. The attendance on Day-1 was 260, which included special guests, speakers, sponsors, invitees and organizers and Day-2 also registered a very good attendance of 240 participants. The conference participation has been increasing year after year which substantiates the relevance of the themes being chosen by the Chapter for its annual conferences.

Mr. A. S. Kiran Kumar, Vikram Sarabhai Professor, ISRO and Member, SPACE Commission, Government of India, (Former Chairman, ISRO) was the Chief Guest on Day 1. Mr. Atul Kumar, GM & CIO, Syndicate Bank was the Guest of Honour and Mr. Jose Varghese, Co-Founder, Paladon was the Key Note Speaker.

Mr. V. Jayaraman, GM, Canara Bank was the Chief Guest on Day 2 and Mr. Arun Khannur, Product and Process Quality Consultant was the Key note speaker.

The conference included a plethora of speakers from various sectors of industry presenting on a variety of topics related to the theme of the conference and very positive feedback was received from delegates of the conference.

The Conference sponsors were:

- Gold Sponsors: Canara Bank and Syndicate Bank
- Silver Sponsor: Assertion
- Bronze Sponsors: NERIDIO and CYBERPWN
- Partners: KPMG, QUALYS & TGROUP.

The Session details are provided here below:

- Conference Theme: “Cyber Resiliency in Digital Era”
- Date: 19th & 20th July 2019
- Time: 9.00 AM to 5.30 PM
- Venue: The Taj, MG Road, Bangalore

Day 1: 19-Jul-2019

Welcome address by Conference Chair:
Mr. Satish Kumar Dwibhashi, Vice President, ISACA Bangalore Chapter

Inauguration: Lighting the Lamp by Chief Guest, Guest of Honour, Key Note Speaker, President & Vice President

Address by: Mr. Sridhar S., Chapter President

Inaugural Address by: Chief Guest - Mr. A. S. Kiran Kumar, Vikram Sarabhai Professor, ISRO and Member, SPACE Commission, Government of India, (Former Chairman, ISRO)

Guest of Honour Address: “Resiliency and Regulations” - Mr. Atul Kumar, General Manager & Chief Information Officer, Syndicate Bank

Key Note Address: “Cyber Resiliency Fair Warning - You cannot build this in a day” - Mr. Jose Varghese, Co-Founder, Paladon

Release of Conference Edition Newsletter: Newsletter was released by the Chief Guest

Felicitation of High Scorers in the ISACA Certification Exams: Felicitated by Chief Guest

Vote of Thanks: Ms. Vijaya Vanitha, Director, Programs, ISACA Bangalore Chapter, proposed vote of thanks.

Technical Sessions:

- Session 1: “Cyber Defense vs Cyber Resiliency” - Mr. Arand Trivedi, Cyber Security Business Head, TUV SUD, Mumbai

- Session 2: “Cyber Security Audit” - Mr. T. R. Rajesh, Associate Director, IBM
Session 3: "A proactive approach towards Cyber Resiliency" - Mr. Narasimhan Elangovan, Partner of KEN & Co

Session 4: “Asset Visibility in Modern IT” - Mr. Debashish Jyotiprakash, Solutions Director, SAARC & APAC, Qualys

Session 5: "Application Security Posture" - Mr. Sreekanth Nemani, Director, ASSERTION

Session 6: “Privacy & Trust Engineering” - Mr. Ricky Jha, T Group - Founder and CEO

Panel Discussion: "Cyber Resiliency in Digital era" - Anchor - Mr. Raghv RV, Past President, ISACA, Bangalore Chapter

Panel Members:
1. Mr. Peter Cheechoo - VP & CTO, NERIDIO
2. Mr. Debashish Jyotiprakash - Solutions Director, SAARC & APAC, Qualys
3. Mr. Vinod Thomas - President, Venture Been Consulting
4. Mr. Anand Trivedi - Cyber Security Business Head, TUV SUD, Mumbai
5. Mr. Satish Kumar Dhillon - VP, ISACA Bangalore Chapter & CISO, Wibmo Inc.

Delegates: 260 CPE Hours: 7

Day 2: 20-Jul-2019

Opening Remarks: Mr. Sridhar, President, ISACA, Bangalore Chapter

Address by Chief Guest: Mr. V. Jayaraman, General Manager, Canara Bank

Key Note Address: Mr. Arun Khanna, Product and Process Quality Consultant

Technical Sessions:

Session 1: “Cyber Resiliency Audit” - Mr. Rajiv Gupta, VP & Head of Internal Audit, Diageo India

Session 2: “Cyber Risk Insurance” - Mr. T. L. Arunachalam, Director, Bharat Re-Insurance Brokers, Chennai

Session 3: "Cyber Resilience - From a Bottom up Perspective" - Mr. Peter Cheechoo, VP & CTO, NERIDIO

Session 4: “Cyber Resilience in the Digital Era” - Mr. Merrill Cherian, Director, KPMG India

Session 5: “Cyber Resilience in the Digital Era” - Mr. Deepak Shukla, AGM, Canara Bank

Session 6: “Digitas Era - ‘BCM to Operational Resilience” - Mr. Prashant Choudhary, Partner, E&Y

Session 7: “Role of GRC professionals in Digital Era” - Mr. Abdul Rafiq, MD, Wincer Infotech Ltd.

Vote of Thanks: Mr. Velmuruga Venkatesh - Director (Marketing), ISACA Bangalore Chapter, proposed vote of thanks.

Delegates: 240 CPE Hours: 7

The conference was well appreciated and received positive feedback.

CPE Meetings:

2. Topic: “Understanding the Cloud and Security requirements”

Venue: Web Based Session

Date: 24-Aug-2019 Time: 6:00 PM - 8:00 PM

Session Abstract:

The CPE session has given an overview and introduction to cloud, different cloud service models, deployment models, major cloud service providers, the benefits/advantages/disadvantages of cloud deployment, current workload movement to clouds, cloud ecosystem, security requirements, current exposures and roadmap of cloud in the future.

Speaker profile:

T R Rajesh is an Information Security Professional with more than 22 years experience in the IT industry. TR has diversified experience from the delivery to compliance, risk management to auditing, architecture and management for Information Security domain and professionals. He is a regular speaker for ISACA Bangalore Chapter and is working with IBM as an Associate Director and India/SA Chief Security, Regulatory and Risk Officer. TR is an MBA with Doctorate in Management Studies, CISA, CISM, TOGAF, CCSE, ISO27001 LA, ISO3000LA, COBIT(5), ITIL (Foundation, Intermediate - 50).

CPE credits: 2 Hours of CPE credits awarded

Total Participants: 104

Positive feedback was received and appreciated by all participants.
2. Topic: “Understanding Next-Gen SOC - Security Operations Center”
   Venue: Web Based Session
   Date: 14-Sep-2019 Time: 6:00 PM - 8:00 PM

Session Abstract:

The CPE session provided the attendees with an overview and introduction to SOC - Security Operations Center and the need for organizations to improve detection, response and recovery capabilities. Cyber-attacks are increasing in sophistication and for effective mitigation, organizations are building next-generation SOCs with next-generation SIEM solutions and taking it to the next level with SOAR (Security orchestration, automation and response) platforms.

Speaker profile:

Satish Kumar Dwibhashi, with over 28+ years of experience in IT & Information Security currently plays the role of CISO for a FinTech company Wibmo. He is certified on CISA, CISM, CRISC, CGEIT, CBCI, ISO 27001 Lead Auditor & Implementer, COBIT 5 Foundation & Implementer, an active Platinum member of ISACA and enjoys teaching and mentoring. He has been actively volunteering for more than a decade and is currently the Vice President & CSX Liaison at ISACA Bangalore Chapter. He is a regular speaker at various events, forums and provides thought leadership.

CPE credits: 2 Hours of CPE credits awarded.

Total Participants: 105

The session was much appreciated by all participants.

Supported Events:

Two courses of 5 days each ISO 27001:2013 based Lead Auditor Training course organized by Certification Partner Global (formerly known as ISC Global).

Date: 24th to 28th July 2019 (Wednesday to Sunday) and 24th to 28th Sep 2019 (Tuesday to Saturday)

Venue: HOTEL PAI VICEROY, 1504, 16th Cross, 9th Main, 3rd Block, Jayanagar, Bangalore, Karnataka - 560 011

Time: 8:30 AM to 5:30 PM

ISACA member participants earned credit of 35 CPE hours in accordance with ISACA Guidelines. Also got substantial discount against their registration fees.

Instructor: Exemplar Global Accredited Instructors -

For the course from 24th to 28th July 2019


For the course from 24th to 28th September 2019


Public Introductory Seminar on ISACA Certification Courses:

One Intro Seminar on ISACA Certification Courses was conducted by the Chapter during the quarter.

1. Venue: Trinity Isle Hotel, Bengaluru - 560 020
   Date: 10-Aug-2019 Time: 5:00 PM - 7:00 PM

The representatives from the chapter imparted an overview on all ISACA Certification Courses - CISA, CISM, CGEIT, CRISC & Cyber Security Nexus to the participants. The Chapter also distributed the certification brochures during the seminar.

There were 34 aspirants and the program was well appreciated and received by participants.

Review Classes:

The Chapter has conducted 1 batch of CISA classes on 5 Sundays and 1 batch of CISM classes on 4 Saturdays for 24 aspirants in August and September 2019. Also conducted 1 batch of 5 Days CGEIT classes for aspirants which is spread over in September and October 2019.

Plans for the quarter - October - December 2019

1. CPE Meetings on alternate Saturdays
2. One batch of 4-5 weekend CISA, CISM, CRISC and CGEIT review classes in November/December 2019
For Registrations, contact the Chapter Office @ 080-50030042 / 23377956 or write to chapter@isacabangalore.org. You may complete the registration format given below and mail the word document with particulars of fee payment (Also you can register on the first day too at the Chapter Office. Please walk-in with a cheque by 8.30 AM to complete registration formalities).

3. A 2 Day hands on COBIT 2019 workshop.

4. Annual General Meeting of the Chapter on 19th October 2019:

Twenty Third Annual General Meeting of the Bangalore Chapter of ISACA will be held from 5.00 PM to 8.00 PM on Saturday the 19th October, 2019 at Hotel Trinity Isle, Swastik Circle, 139, Subedar Chatram Road, Seshadripuram, Bangalore - 550 020 to transact the following business:

**Agenda:**

1. To approve the AGM Minutes of 2018
2. To consider and adopt the 23rd Annual Report
3. To consider and approve Audited accounts for the year ended 31st March 2019
4. To appoint statutory auditors for the year 2019-2020 and fix their remuneration
5. To Elect Executive Committee Members (EC members) for the Executive Committee for the year 2019-2020 (Elections will be held, if required)

**NOTE:**

i. Members who have opted for affiliation to Bangalore Chapter and whose membership is valid and current as on 30th June 2019 are eligible to participate in the AGM.

ii. Members are requested to bring their identity card (or any other proof indicating their membership status) and copy of the Annual Report to Annual General Meeting.

iii. Members who wish to send their nomination for elections to the Executive Committee (EC) are required to submit nomination form, duly filled in, at the chapter office.

iv. Rules, procedures and application to file nominations for the EC 2019-2020 are available at chapter website http://www.isacabangalore.org

v. Last date for submission of the nomination is 7th October, 2019 (Monday) before 5.00 PM.

vi. Last date for withdrawal of nomination is 9th October, 2019 (Wednesday) before 5.00 PM.

vii. Announcement of the final list of candidates contesting for elections 14th October 2019 (Monday).

viii. Announcement of elected candidates is 19th October, 2019 (Saturday).

ix. Members are requested to write to the chapter office one week in advance with regards to any clarifications required related to the Chapter’s annual report, the Financials statements, etc.

Further, ISACA Bangalore Chapter announces special CPE session on the day of Annual General Meeting, the details of which will be intimated through mail to members.

---

**The 2010s: A Decade of Growth and New Focal Points for ISACA**

**ISACA Now**

**Posted:** 9/24/2019 2:58:00 PM by ISACA News | **Category:** ISACA

The 2010s have seen remarkable growth at ISACA. From the debut of the CRISC certification to the addition of the CMMI Institute to the creation of the Sheffield Tech program and the added emphasis on providing cybersecurity resources, as underscored by the launch of the Cybersecurity Nexus (CSX), we are drawing near to the close of what has been a dynamic decade in ISACA’s 50-year evolution.

"You see the importance of the work ISACA is engaged in more than ever," said member Erik Rolland.

Added MariosDamianides, 2003-05 ISACA board chair: "It's been terrific to see that adaptability and that forward-thinking."

Find out more about ISACA's arc in the 2010s on ISACA's 50th anniversary site in a recently released video: "ISACA in the 2010s and Beyond."


---

7
ISACA Bangalore Chapter
Registration Form for CISA & CISM for
Computer Based Exams in 2019

November / December, 2019 4th Batch

Venue: Chapter Office - Address mentioned underneath

1. NAME: .................................................................................................................................................

2. ☐ CISA ☐ CISM ☐ CRISC ☐ CGET (Please tick for Registration)

3. ISACA MEMBERSHIP NO: ........................................................................................................... NON MEMBER (Please tick as applicable)

4. DESIGNATION: .............................................................. QLFN: ............................................................

5. ORGANISATION: ................................................................................................................................

6. ADDRESS: ...........................................................................................................................................

.............................................................................................................................................................

 .............................................................................................................................................................

7. PH:OFFICE..................................................RES........................................................MOBILE:......................................................

8. EMAIL: ...............................................................................................................................................

9. PRESENT WORK AREA : ......................................................................................................................

Registration Fee per batch classes: Rs. 8500/- for ISACA Members and for Non members Rs. 9500/- (Inclusive of Taxes) A Local Cheque/Bank Pay Order in favour of ISACA, Bangalore Chapter and the same may be despatched to the Office address

or

NEFT (Wire transfer) to : State Bank of India, PBN 1027, 14th Main, 1st Block, Rajajinagar Branch, Bangalore-10. Savings Bank Account No.54003825745. Account Holder : ISACA, Bangalore Chapter
IFSC Code: SBIN0040197 / MICR 560002408

Date_________________________ Candidate Signature

Course Material - Received / to be received.

No.5-13, 531/A, 2nd Floor, Priya Chambers, Dr. Rajkumar Road, Opp. St. Theresa’s Hospital, 2nd Stage, Rajajinagar, Bangalore - 560 010, Ph: 080 55640042 / +91 9535197405
Email ID: chapter@isacabangalore.org. Website: www.isacabangalore.org
Mapping ISO 27001:2013 to HIPAA Requirements - Administrative, Technical and Physical safeguards of HIPAA to various ISMS controls.

Profile details:
Mr. Kumar G. S. has a total of 20 years experience, of which, ten years is in Information Security, Risk Management, Business Continuity, US healthcare Compliance with HIPAA and HITECH knowledge. He is an MBA in Total Quality Management and has the following professional Certifications/Qualifications as below : CISM Certification in 2017, Lead Auditor In ISO 27001:2013, ISO 9001:2015, CEH V10, ITIL V3.0

Post Graduation certification in Cyber Law from Symbiosis Centre for Distance Learning (one year certification course)
He is currently pursuing Cloud Security training.

"Proper Implementation of ISO 27001:2013 (ISMS), boosts your assurance to meet majority of the important requirements of US Healthcare act – HIPAA."

With the last one Decade of exposure in Healthcare Information Security and Client Contractual requirements, I just thought of sharing my Healthcare IT and IS knowledge with ISACA Fraternity.

If you are working for a US Healthcare Covered entity as - Providers or Clearing Houses or Payers or Business Associate, then HIPAA Compliance applies to you.

As per HIPAA Omnibus Rule 2013 the BA (Business Associate) organization is equally responsible to safeguard the clients/end customers’ PHI and PII like covered entity.

For the easy monitoring and reference, I have mapped majorly 45 CFR 164.308, 164.310, 164.312, 164.314 and 164.316 requirements to ISO 27001:2013. (the detailed mapping of ISO 27001:2013 to HIPAA and NIST is available at HHS website).

The graph does not include all sections of HIPAA, refer HHS for other sections and clauses and adherence.
Basic requirements:

An organization, which has defined, documented, implemented and tested all the IS policies and procedures can adhere to other acts and requirements like HIPAA, HITECH and PCI-DSS.

The implementation of below IS policies provides assurance to the clients and organization:

1. Information Security policy
2. Information access control policy
3. Human Resources Security Policy
4. Incident Management policy
5. BC/DR policy: Business Continuity and Disaster Recovery Policy
6. Business Associate Agreement (BAA)
7. Physical Security and Environmental policy
8. Information Backup policy
9. Asset Management, Information Classification and Asset Labelling policy
10. User Acceptable policy
11. Password Management policy
12. Encryption policy
14. Legal policy on adhering to various local and international Laws
15. Data retention Policy and Media Disposal Procedure

Overview about Business Associate:

What is a “Business Associate?” A “business associate” is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.

A member of the covered entity’s workforce is not a business associate. A covered health care provider, health plan, or health care clearinghouse can be a business associate of another covered entity.

The types of functions or activities that may make a person or entity a business associate include payment or health care operations activities, as well as other functions or activities regulated by the Administrative Simplification Rules.

Key Note:

- Legal and Regulatory requirements should always be verified in the authorized websites before conclusion considering the periodic Legal updates
- Each organization can go for individual assessment of ISO 27001:2013 and HIPAA separately based on senior management decision and business needs.
- Refer https://www.hhs.gov/- the United States Department of Health & Human Service website for updated information and mapping of HIPAA to other standards.

Source:


https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html


ISO 27001:2013 standard

CPE On Demand

Gain new understanding and earn additional Continuing Professional Education (CPE) hours on your schedule - anywhere you have hi-speed Internet access. Connect with ISACA's CPE On Demand to stream video of invaluable, expert-led presentations recorded live at global conferences and training events. Choose from information systems topics that best fit your role and goal:

- CPE on Demand: All Access
- CPE on Demand: Data Security
- CPE on Demand: Emerging GRC Challenges
- CPE on Demand: Security Practices for Business
- CPE on Demand: Technical Security Insights
- CPE on Demand: Third-Party Services

Courtesy: http://www.isaca.org/Education/On-Demand-Learning/Pages/default.aspx
Auditing Green IT Governance and Management With COBIT 5

Today's organizations find themselves facing a relatively new challenge—governing and managing sustainability—since sustainability has become an important issue and is increasingly essential for business. Green IT practices help enterprises achieve and maintain environmental sustainability. Like any other business practice, green IT can be optimized for value—not only to the business, but also to the broader community—when it is appropriately governed and managed. COBIT® 5 offers an IT governance and management framework to help enterprises standardize and control green IT, so that it meets the expectations of the business. The case study herein offers one example for planning and conducting, green IT audits to measure the enterprise's progress toward green IT goals.

Understanding Green IT

Green IT reflects a broad array of technology and practices that help enterprises conserve energy and natural resources, reduce or eliminate waste, reuse, recycle or repurpose materials, especially technology hardware and its infrastructure and design, implement and use information systems sustainably.

Green IT not only strives to reduce the negative impact of IT departments have on the environment, but also seeks to use information and technology (IT) in ways that reduce environmental impact more broadly. Green IT, therefore, spans two overlapping but distinct conceptual domains:

- **Green in Information technology (green in IT)**
  As a producer of goods and services, enterprise IT itself has an impact on the environment. It

---

J. David Patón-Romero, CISA, PMP
Is a Ph.D. student in advanced information technologies at the University of Castilla-La Mancha (Spain), and computer science and mathematics at the University of Bari Alba More (Italy). He is also a consultant/supervisor at the accredited laboratory for software quality assessment AOC Lab. His research interests include governance, management, and auditing at green IT.

Manuela Baldassarre, PMP
Is currently an assistant professor at the University of Bari Alba More (Italy) and a partner at Software Engineering Research and Practices. Her research interests lie in empirical software engineering, harmonization of multiple improvement models, quality assessment and improvement in software. She collaborates on several research projects and carries out consulting and in-field experimental with a small and medium enterprises. She is a partner of the SER and Practices spin-off company. Currently, she is the representative of the University of Bari in the Italian Software Engineering Research Network (SERIN) and involved in various program committees related to software engineering and empirical software engineering international conferences.

Moisés Rodríguez, CISA
Is the chief executive officer (CEO) of the accredited laboratory for software quality assessment AOC Lab.

Mario Piattini, CISA, CRISC, CISM, CGBIT, PMP
Is full professor at the Escuela Superior de Informática of the University of Castilla-La Mancha (Spain). He leads the ALARCOS research group and his research interests include software engineering and information system quality.
contributes energy and technology artifacts (including both hardware and software), produces emissions, etc. Therefore, IT departments can implement green IT (more consumption and consume more sustainably.

Green by information technology (green by IT)— As an enabler of efficient and sustainable practices, information and technology (IT) can provide tools—the number and scope of which are virtually limitless—that facilitate sustainability outside the IT department, across the enterprise and beyond.

Auditing Green IT

Enterprises today often audit green IT from a business perspective rather than technical perspectives. It is critical to distinguish between these approaches: Representing the business to customers and/or the general public, in terms of sustainability is often a primary goal (i.e., reputation with respect to sustainability), compared with optimizing green IT practices at the operational and technical levels. Enterprises often regard reputation as a primary driver of business benefit. Figure 1 summarizes the different objectives for conducting a green IT audit.

The scope of green IT audits is determined by the nature of the audit, whether green by IT or green in IT.

If the audit evaluates sustainable practices implemented and/or executed in IT and intended to reduce the negative impact on the environment of IT itself, the audit is composed of a green IT audit, and the scope is reduced to the IT department.

If the audit evaluates sustainable practices implemented or facilitated by IT and intended to reduce the negative impact on the environment of other systems or businesses, the audit is composed of a green by IT audit. Furthermore, the scope will encompass information and technology that are used for these purposes, as well as the systems and disciplines that are affected by them.

A Model Green IT Audit

An IT services center (USC) in Mexico offers an ideal model for the green IT audit. Both the USC and the broader university are committed to sustainability and green IT. In fact, green IT is one of the university’s main disciplines and a critically important pillar within the USC. The university established a dedicated division and program for sustainable initiatives and the USC pursues continuous green innovation and improvement. Figure 2 lists some of the USC’s green IT practices prior to the audit.

Initially, the USC implemented green IT practices independently, without following any framework, in

<table>
<thead>
<tr>
<th>Figure 1—Green IT Audit Objectives</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Level</strong></td>
</tr>
<tr>
<td>Business</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Operational</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Technical</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
Figure 2—Model Green IT Practices of Audit Subject USC

<table>
<thead>
<tr>
<th>Domain</th>
<th>Practice</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green IT</td>
<td>Implementation of cloud services</td>
<td>Use services through Google Cloud</td>
</tr>
<tr>
<td></td>
<td>Use of recycled paper for printing and photocopying</td>
<td>Computer equipment deregistered and sent for recycling, e.g., computers, servers, tablets, monitors</td>
</tr>
<tr>
<td></td>
<td>Special handling of batteries</td>
<td>Treatment of deregistered computers; disassembly of parts and classification for later recycling</td>
</tr>
<tr>
<td></td>
<td>Special handling of computer equipment, which is deregistered and sent to specific destinations for treatment</td>
<td>Implementation of cloud services; hardware reuse, e.g., hard drives, graphics cards, memories</td>
</tr>
<tr>
<td></td>
<td>Reuse of hardware from obsolete equipment</td>
<td></td>
</tr>
<tr>
<td>Green IT</td>
<td>Implementation of cloud services, issuance of digital certificates/documents</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Implementation of cloud services, registration and evaluation of academic projects electronically</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Implementation of cloud services, issuance of digital vouchers for administrative services</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Digital vouchers for administrative services</td>
<td></td>
</tr>
</tbody>
</table>

The absence of a global standard. After the adoption of the application of COBIT 5 for green IT, the USC had a framework to follow.

The model audit was intended not only to evaluate, but also to help standardize USC practices relative to COBIT 5. Because the USC implemented both green-in-IT and green-by-IT practices, the model audit proceeded along dual tracks, and (in both cases) the first two levels of the maturity model shown in Figure 3 with the example of the green in IT audit questions of the process BA02: Manage assets.

The audit of the first two maturity levels (of both green-in-IT and green-by-IT tracks) identified certain strengths, and opportunities for improvement in each of the processes audited (Figure 4).

After analyzing results for the audited processes and considering the maturity model, auditors determined that the USC partially achieved level 1 maturity in both the green-in-IT and green-by-IT tracks. Figure 5 illustrates by way of example detailed results for the green in IT track.

To determine the level of compliance of each COBIT 5 process, auditors evaluated a series of activities.

Figure 3—Green in IT Audit Questions for the BA02 Process

<table>
<thead>
<tr>
<th>Process</th>
<th>Audit Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>BA02: Manage assets</td>
<td>Are all the assets of green in IT identified and registered, along with the requirements that they cover and the relationships and dependencies between them?</td>
</tr>
<tr>
<td></td>
<td>Are the critical assets of green in IT classified according to their level of criticality?</td>
</tr>
<tr>
<td></td>
<td>Are the requirements and guidelines for the use of the assets of green in IT satisfied throughout their whole life cycle?</td>
</tr>
<tr>
<td></td>
<td>Are the costs derived from the assets of green in IT evaluated?</td>
</tr>
<tr>
<td></td>
<td>Is there a license management system for software related and/or affected by green in IT?</td>
</tr>
</tbody>
</table>

© 2019 ISACA. All rights reserved. www.isaca.org
Figure 4—Strengths and Opportunities for Improvement in Green IT for Audit Subject USC

<table>
<thead>
<tr>
<th>Strengths</th>
<th>Opportunities for Improvement</th>
</tr>
</thead>
<tbody>
<tr>
<td>High level of commitment and awareness of all USC members and stakeholders with regard to ecologically sustainable and green IT.</td>
<td>Implementation of green IT practices has been carried out following the organization's own criteria and a series of isolated independent best practices; it is highly recommended to adopt and establish some framework or standard to guide implementations throughout the life cycle, which will increase level of success and foster improvement.</td>
</tr>
<tr>
<td>Implementation of a significant number of sustainable practices.</td>
<td></td>
</tr>
<tr>
<td>Compilation of official documents that endorse ecologically sustainable (e.g., policies, strategies, objectives).</td>
<td></td>
</tr>
<tr>
<td>Existence of a program dedicated to ecologically sustainable, which includes internal sustainability in all its aspects, provides awareness and training, and manages all aspects related to the environment and green IT.</td>
<td></td>
</tr>
<tr>
<td>Continuous evaluation of performance, effectiveness, costs, etc., reporting of status, results, monitoring, etc., corrective actions regarding all aspects that affect or are affected by ecologically sustainable and green IT.</td>
<td></td>
</tr>
</tbody>
</table>

Figure 5—Compliance of Audit Subject USC to Green IT Process Maturity Levels

1. **Level 1**:
   - BA03 Manage Assumptions
   - D501 Manage Operations

2. **Level 2**:
   - AP002 Manage Strategy
   - AP003 Manage Outcome and Costs
   - AP012 Manage Relationships

3. **Level 3**:
   - AP007 Manage the IT Management Framework
   - D500 Manage Configuration

4. **Level 4**:
   - AP007 Manage the IT Management Framework
   - AP003 Manage Outcome and Costs
   - AP012 Manage Relationships

5. **Level 5**:
   - ED030 Ensure Risk Communication
   - ED040 Ensure Business Continuity
   - AP001 Manage the IT Management Framework
   - AP003 Manage Outcome and Costs
   - AP007 Manage the IT Management Framework
   - D500 Manage Configuration
that are specific to green IT (defined during the auditors’ prior exercise adopting COBIT 5 to green IT) for compliance with the practices and processes that COBIT 5 establishes. Compliance with green IT activities indicates that processes are fulfilled and, therefore, each related process is also fulfilled. Where the USC did not fully comply with green IT activities, the auditors indicated possible solutions to achieve compliance. For example, with respect to process BA09 Manage assets, auditors identified the deficiencies shown in figure 6.

Based on figure 5, it is clear that for the USC to meet maturity level 1, it must fully comply with process BA09.

Conclusion

Green IT is not a utopian ideal. It is real, and it is here to stay. It provides great benefits to organizations, society and the environment. Green IT still has not been acknowledged to the degree it deserves—and there are not enough frameworks and standards to help enterprises understand and implement it. The standards and frameworks developed by ISACA, such as COBIT 5, are appropriate and adaptable to integral practices such as green IT. Armed with appropriate standards and frameworks, auditors can be the engine of change for sustainability in and by IT.

Endnotes


<table>
<thead>
<tr>
<th>Deficiencies</th>
<th>Possible Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>The critical assets of green IT are not documented or registered (i.e., the criticality of each is known). Because they are not documented, and despite known criticality, there may be no expectations, which could be solved if everything were registered.</td>
<td>Identify the critical assets of green IT and classify them in an official document according to the level of criticality that each one has.</td>
</tr>
<tr>
<td>The software that is used is provided through “Google for Education” which is free for educational purposes. However, even if it is free, the USC should investigate the compliance of this software with sustainability and label it as sustainable software (when applicable) in the download ports and include official documents, which will help decision making when acquiring software.</td>
<td>Label as “green” (sustainable) the software related or affected by green in IT.</td>
</tr>
</tbody>
</table>

© 2019 ISACA. All rights reserved. www.isaca.org

ISACA JOURNAL VOL 4

Courtesy: ISACA.org/Journal/Archives/2019/Volume-4
The Pain of Automation
Internal Audit Functions Face Real World Challenges Amid Optimistic Environment

Internal audit leaders are looking at automation technologies for many of the same reasons as business management. Automated processes can run in the background, allowing auditors to focus on more important issues than they could manually. Also, deviations from expected or acceptable controls can be brought to auditors’ attention more quickly (in near-real-time) than if they were audited manually. Advantages such as continuous monitoring, automation of repetitive processes, and the ability to audit large populations (as opposed to sampling) offer internal audit departments the opportunity to expand their view, discover new limited resources, and, most important, provide greater value to the enterprise.

In light of these possibilities, optimism around automation in internal audit is understandably high. In a recent survey, nearly half of US risk and compliance professionals, internal auditors, executives, and board members surveyed said their organization planned to modernize its compliance function in the next 12 months. However, according to another study, just 14 percent of internal audit functions could be considered advanced in their technology adoption (including the use of robotic process automation [RPA]) to expand the expediency and coverage of their audits, while 30 percent are either adopting advanced technologies at a slower pace or not at all.

These findings suggest that, in spite of the promised benefits of automation, internal audit departments are encountering hurdles on the path toward realizing these benefits. Three of the key challenges are:

1. Integrate RPA into audit processes and job functions.
2. Ensure that new automated processes are compliant with standards and regulations.
3. Strategically address the impact of automation on the audit function as a whole.

Process Identification and Selection
One of the fundamental challenges internal audit departments face in implementing RPA is choosing the process, or processes, to be automated. It is not always obvious what the department should focus on or prioritize.

For example, applying a risk-based approach might point toward investing resources in developing RPA based on the areas of greatest risk to the organization. If the internal auditors are looking at an area of critical risk, the thinking goes, then they want to maximize the effectiveness of the audit processes they are using to perform that role.

On the other hand, some audit functions would rather focus on automation efforts on those audit processes that have the greatest potential for efficiency. Within the internal audit function, in this line of thinking, if automation efforts focus on automating the least valuable and/or least efficient, processes to free up auditor capacity, it allows the department to do more across the board with finite resources.

Wade Cassels, CISA, CFE, CIA
is a senior IT auditor at Nielsen. He supports Nielsen’s IT general controls, internal audit engagement and the audit recording and re-examination functions for Nielsen Internal Audit.

Jane Traub, CISA, CIA
is an internal audit director at Nielsen. She leads internal audit automation initiatives, manages audit engagements, and the Global Media team and supports compliance with the Code of Conduct.

Kevin Alvero, CISA, CFE
is a senior vice president of internal audit, compliance and governance at Nielsen. He leads Nielsen’s internal quality audit program and its industry standards compliance initiatives, supporting the company’s global media products and services.

Jessica Fernandez, CISA
is an internal audit vice president at Nielsen. She leads all internal and external audit engagements around Nielsen’s Digital and Advanced TV products and services.
Further complicating the choices is the fact the internal audit department may not be solely responsible for making the selection. If the department is participating in a larger organization-wide automation initiative, people outside the department may have a say in what processes are chosen for automation.

Even if the organization has a well-conceived system in place to select processes for automation, a good set of performance measures and an initial set of performance measures is also needed to inform that system and accurately assess which processes will have the greatest return on investment (ROI). Many organizations do not have sufficient performance data, and that can lead to the risk of automating the wrong things.

Most likely, though, the decision is going to come down to money saved. This is important for internal audit departments seeking funding and support for automation efforts. The better they can make the ROI case and quantify the benefits of automation in terms of cost savings, the easier it will be to justify their selection of processes to automate.

In addition to ROI potential the process in question must have reliable, quality input. The quality and reliability of the data input into an automated process is the single greatest determinant of whether users will be able to trust its output.

Many internal audit functions will look at the processes they currently perform and choose automation for those that RPA can help them do better. However, that is not necessarily the best approach. Audit functions can fall into the trap of simply retrofitting old procedures with new technology to make them incrementally better. Ideally, audit functions should look at how RPA can help them adopt new capabilities to deliver value to the organization that they could not previously.

Whether looking at new or existing processes, internal audit departments that are trying to build momentum on the path toward automation should look for processes that:
- Has a clearly definable ROI
- Relates to an area of key business risk to the organization
- Has reliable, quality inputs
- Is labor intensive, subject to human error and generally inefficient

These are the areas internal audit should target first, and formalized RPA projects should focus on a limited number of high-impact targets to preserve momentum.

Solution Development

Even though a process may be an ideal candidate for RPA in theory, actually developing the technology to automate it can present numerous challenges. When it comes to artificial intelligence (AI) and robotic process automation (RPA), one of the key hurdles for internal audit departments to overcome is simply making sure everyone is aligned in terms of what it is they are talking about. AI, in simple terms, involves a program that takes data patterns and learns from them to make informed decisions based on learned rules. An example would be suggesting items to buy from a website that is used regularly for purchases by a consumer. People may be tempted by a message such as “You might also like...” This concept extends to the business world, where established patterns of business processes can apply AI to predict future behavior and note exceptions to anticipate behavior of systems or people. RPA, by contrast, is often used where a process does not need decision-making to execute. It uses software programs, often called “bots,” that mimic a human’s behavior such as sequential steps in data collection, report issuance, or any repetitive, systematic, rule-based process.
of the aspects of third-party risk management, including service level agreement (SLA) and security/confidentiality, come into play. In particular, ongoing updates and maintenance will be tied to the vendor solution going forward, and it may not be feasible to bring these in-house once a customized automation process is established by the vendor; so the internal audit department should understand the ongoing requirements just as well as the upfront ones. Plus, the internal audit department must ensure that needs are accurately defined and scope is carefully managed to avoid implementing a more powerful and, thereby, costly solution than is absolutely necessary. Weighing and balancing these trade-offs is important to do prior to committing to a course of action for automation.

RPA experts insist that robots do not make mistakes and, if they are programmed correctly, RPA technologies have great potential to save auditors’ time through the automation of routine, repetitive, rule-based actions. However, if they are programmed incorrectly or incomplete, or are altered, errors can be introduced during the automated process. These process automation errors can perpetuate larger, systemic errors to a greater degree than similar manual processes. Therefore, whether the solution is being developed in-house or by a vendor, clear documentation of each step and rule in the processes to be automated and verification of bot functionality must be performed before implementation of RPA, and it is important to understand the demands this will place on internal audit resources before the solution development process begins.

Throughout the solution development process, internal audit automation leaders should also remain aware of their alternatives. A fully customized, fully automated solution may, in fact, not be the ideal solution for every automation project. For example, if 30 percent of the process in question can be automated fairly easily, but the remaining 20 percent would come at a high relative cost, then automating the 80 percent may be the ideal solution for the department’s needs. Indeed, “full automation” can be undesirable based on the application. Processes that involve decisions that humans need to make are not suited to total
automation. RPA is not the only mode of automation, either. Replacing legacy systems or building powerful application programming interfaces (APIs) into legacy systems may allow organizations to automate processes with less effort than building RPA solutions, and those leading automation efforts should avoid fixating on RPA alone for automation.

Finally, the solution development process should not be confined to the internal audit staff and restricted to the technology experts who are writing software. It is critical that internal audit departments integrate the intended users of the solution into the development process and train them because, for one thing, a person has to be able to evaluate when an automated output is wrong. The audit functions most advanced in their use of technology are developing their people and processes at the same time. Not only should people be trained on how to utilize an RPA solution, but it is also critical that they understand the benefits from a strategic perspective. If these are not explained properly, the concept can generate anxiety (e.g., “Will these software robots be taking away our jobs?”). These teams can contribute to inertia for launching RPA projects. In any automation effort, the benefits of less time spent on tedious, repetitive tasks and freeing up staff time to focus on value-added activities should be communicated early and often to all stakeholders.

Garbage In, Garbage Out

While internal audit departments generally do not have the expertise to develop technology solutions in-house, they still play a critical role in the ultimate success of an automation solution based on how well they educate the software developers about their needs and objectives throughout the project, not just at the beginning. The usefulness of a technology solution will directly correlate to the ability of the business process owners and subject matter experts to explain, step-by-step, how a process is conducted, from end to end. If the internal audit department does not take care to articulate its needs thoroughly and accurately, then the resulting technology solution will not succeed. Screenshots and/or screen video recordings of staff performing the actions can be helpful in this process. Templates and completed examples are also useful ways to smooth the discovery and evaluation phases of potential automation projects. Before coding, technical review by those responsible for writing the actual programming code is also necessary input. Having dedicated outreach staff for organizationwide automation initiatives is also helpful for disseminating information about what RPA can and cannot do for enterprise teams.

Process Interactions

Evaluating a process for automation on its own merits can be complex enough, but it is often compounded by interaction with other areas. Robots (in the RPA context) are entirely technology agnostic and can be used with any application, so they can work across functions and across applications.

"EVALUATING A PROCESS FOR AUTOMATION ON ITS OWN MERITS CAN BE COMPLEX ENOUGH, BUT IT IS OFTEN COMPOUNDED BY INTERACTION WITH OTHER AREAS."

However, a process’s interactions may not be purely technological. For example, considerations must be made for legal and regulatory compliance. At one internal audit shop, the team was motivated to work toward automating a process that consisted of collecting field audit data manually on paper forms. As they set about developing an electronic form that could be completed on a tablet device and then uploaded to a cloud storage drive where the structured data could be used for enhanced analysis, they encountered a roadblock when they discovered that their plan conflicted with the organization’s policy prohibiting the transmission of personally identifiable information (PII) on the cloud.
storage drive, and alternative approaches had to be considered.

Another aspect of process interaction is that if internal audit departments are seeking to automate processes related to specific areas of the enterprise's business, then they must consider the risk of those solutions becoming obsolete if the business changes. When the business changes, the people on the internal audit staff can be assigned to go audit something else, but repurposing a technology solution designed to perform one task and having it perform another may not be as straightforward. This means that internal audit functions should have alignment with business management regarding strategy before pursuing automation initiatives that are tied to the internal audit of a particular area of business.

Conclusion

The potential benefits of automation to internal audit are real and well documented. Just as real, but perhaps less well documented, are the hurdles internal audit departments face on their way to realizing the benefits of automation.

Success begins with choosing the right process to automate and continues with the meticulous documentation and mapping of the current process and defining the requirements of the automation technology to ensure that it works and meets the needs of the users. Beyond basic user testing, users should be integrated into the solution development process so they not only understand how to use the tool, but also its strategic benefits and the potential impact of malfunction. Finally, the broader interactions of the process to be automated should be considered to avoid surprises down the road.

With careful planning and evaluation, automation solutions using tools such as RPA have the potential to streamline audit and business processes and make monitoring of controls more efficient. Decisions about what processes to automate should carefully consider benefits, risk and trade-offs. While many processes can be automated, there must be a disciplined prioritization process to choose which should be automated to make these efforts worthwhile.

Endnotes

7. Ibid.
9. Ibid.
10. Campbell, J.: “Intelligent Automation/RPA and Use for Internal Controls,” IFAC Florida West Coast Chapter and West Florida ISACA Chapter Fraud and Security Seminar, 6 December 2018
11. Ibid.
I Know What I Know (If You Know What I Mean)

Ian Cooke, CISA, CRISC, CGEIT, COBIT Assessor and implementer, CFE, CIPRSE, CIPM, CIFT, CIFE, DIGFM, ITIL Foundation, Six Sigma Green Belt

Published: 9/24/2019 4:56 PM | Category: Audit Assurance

Edie Brickell (incidentally the wife of singer/songwriter Paul Simon) had a modest 1988 hit titled “What I Am.” The opening lines of the song contain the lyrics “I’m not aware of too many things. I know what I know if you know what I mean.”

Besides being a nice play on words, the lyrics are quite prophetic; in reality, we all are somewhat restricted by what we know and understand. We, as ISACA members and IT specialists, all know a lot about IT risk and its 3 main categories. Specifically:

- **IT benefit/value enablement risk** - Associated with missed opportunities to use technology to improve efficiency or effectiveness of business processes or as an enabler for new business initiatives

- **IT program and project delivery risk** - Associated with the contribution of IT to new or improved business solutions, usually in the form of projects and programs as part of investment portfolios

- **IT operations and service delivery risk** - Associated with all aspects of the business-as-usual performance of IT systems and services, which can bring destruction or reduction of value to the enterprise

However, the audiences for IT audit reports, most notably the audit committee, tend to be generalists and, well, they know what they know if you know what I mean. I believe it is therefore incumbent on IT audit to educate or at least to offer to educate committee members in this regard.

We can do this by bringing together our understanding and that of our audit committees. This can be done by drawing a line between the 3 main risk categories, the IT risk to the business objectives and the assurance provided. We need to help the committee understand the significance if the report in front of them states that a key in-scope application is not In compliance with the Information Security Management system (e.g., International Organization for Standardization [ISO] 27001). We want them to know what we know, if you know what I mean.

Courtesy: www.isaca.org/journal/Blog

The Role of Ethics in Risk Management

Rajesh Sehrawat, CISA, CSEIT, ISO 20000, ITIL Expert, PMP

Published: 8/13/2019 4:25 PM | Category: Risk Management

Most people are aware of and talking about risk management. However, barring a handful of high-profile and sophisticated IT organizations, for most enterprises, it is more talk vs. the actual implementation of risk management practices. It is a no-brainer that everything in IT should have active risk management practice embedded into it. When done correctly, it ensures service quality and lowers the risk of outages. While authoring my recent ISACA Journal article, “Rethinking Risk: A New Ethics of Enterprise IT,” I conducted an Internet search of “Ethics in IT” to see if it is an issue and to learn whether ethics issues in IT are reported. I only got a few hits and realized that it appears that ethical behavior in IT is neither measured nor reported, except that the “people” factor kept popping up, especially in terms such as “people are our most important asset” and “our people innovate and are best.” However, in my opinion, people are unpredictable and susceptible to political-management pressures, and us-vs-them and an I/we-have-the-best-solution mind-sets. All these factors do not go well with the overall purpose of IT and are detrimental to our dependency on IT services, which are embedded into our lives. Therefore, there is a need for ethical behavior of IT professionals, and it should be part of overall governance and risk management practices. Also, in my personal observation, people follow processes out of fear or fear of non-compliance, and there might be an opportunity for them to believe in the process or control vs. seeing it as a nuisance.

Depending on which industry one is in, a service issue can be as catastrophic as loss of business to loss of lives. Whenever a catastrophic event occurs, organizations go through lessons learned and perhaps find a technology fix but rarely ever fix behavior.

It would be beneficial if management/consultants/auditors started observing trends in behavior. In my opinion, the only way this can happen is by having an unbiased view of how things are being done. This unbiased view should be insulated from departmental politics and management/executive pressure. I would encourage open dialogue when it comes to ethical behavior risk to processes such as change management, incident management, problem management, and architectural-design decisions, not to mention my favorite, adding to vendor/technology pressures. I know this is easier said than done unless management is willing to change itself—hence this process must start at the Risk IT principle “Establish Tone at the Top and Accountability.”

Courtesy: ISACA Journal > Practically Speaking Blog > Posts
Cybersustainability: Ensuring Digital Strategies That Protect Data

Karen Walsh, Jo and Joe Rashke, CRISC, CIPP, CISP
Published: 10/8/2019 8:52 AM | Category: Security

Increasingly, security professionals use language that makes a distinct comparison between our physical environment and our digital infrastructures. We use terms such as "digital ecosystem," "digital footprint," "IT environment," "data leakage," and "data pollution." As data breaches continue to increase in number and severity, we need to begin thinking about how we protect today's data for tomorrow's future digital strategies.

What is Cybersustainability?

Fundamentally, cybersustainability looks at data as a finite resource, similar to a coral reef or fossil fuels. Similarly, we can look at data from both the "prevent from being polluted" perspective and the "preserve the resource" perspective.

Although no official definition of cybersustainability exists, we use the following definition:

- Adopting/maturing digital transformation strategies
- Establishing access and governance policies that promote cyber health
- Continuous monitoring to maintain data privacy/security
- Communicating across stakeholders
- Promoting operational resiliency

Prevent Data Pollution

When we look at cyberecosystems, we discuss the problems associated with data leakage. Data leakage includes a variety of unauthorized data transfers from an organization’s systems, networks, and software, including physical, digital, and intellectual. For example, a user with excess access to information can choose to download the data or remember the data, both of which are considered data leaks.

Data pollution, in this case, means the way in which data can be accessed or changed within a digital ecosystem such that it impacts the information's integrity, confidentiality, and availability. In many ways, this definition aligns with the concept of a leaking underground storage tank. Homes heated with oil often have old, outdated oil storage tanks that leak the contaminant into the soil. In the same way, unauthorized access leaks data into the larger population, undermining privacy.

Preventing data pollution, therefore, requires organizations to control user access to information using the principle of least privilege.

Preserve Data as a Resource

On the other side of our cybersustainability equation, data are also a finite resource we need to preserve and protect. If we compare data to an environmental resource such as a coral reef, the similarities become more tangible. For example, coral reefs and the organisms that live in them must be protected because few of them still exist. They are finite environmental resources. Similarly, non-public personal data are finite resources. People only have one social security number or one birth date.

Protecting data as a resource, therefore, is imperative. Organizations need to protect and preserve non-public personally identifiable information (PII) because data compromises "depletes" the resource.

Protecting and preserving the integrity, confidentiality, and accessibility of data as a finite resource requires organizations not to only monitor for unauthorized external access to PII, but also to monitor access to it.

Why Identity Governance and Administration Enables Cybersustainability

The World Economic Forum defines the 4th Industrial Revolution as a fundamental change in the way people live, work, and relate to one another arising from new technologies that advance the convergence of physical, digital, and biological worlds.

As we evolve our technologies during this new Industrial Revolution, we need to create forward-thinking digital transformation strategies to prevent the pollution inherent in them. We should be learning from the physical environmental pollution created by factories to prevent similar damage to data arising from the 4th Industrial Revolution.

Thus, we need to look to the new perimeter—identity—to shape our digital transformation strategies. Relying on legacy identity management solutions leaves user data at risk. Protecting data as a finite resource and preventing data pollution relies on creating a risk-based, context-aware identity governance and administration (IGA) program.

Unfortunately, managing identity and access becomes difficult for organizations with complex IT ecosystems. Managing the proliferation of user identities—human and non-person—and the inundation of access requests across often disconnected dashboards creates both a human error risk and increased operational cost. To mitigate this risk and decrease these costs, organizations can incorporate intelligent analytics with predictive access capabilities.

Protecting Today's Information for Tomorrow's Technology

As we attempt to meet the rapid pace of modern technological changes, we need to focus on creating forward-thinking digital transformation strategies. We can learn from the mistakes of our predecessors who led previous Industrial Revolutions. By applying environmental sustainability theory to cybersecurity, we can better protect sensitive information in long term and, ideally, prevent our advances from contaminating or depleting data resources.
<table>
<thead>
<tr>
<th>Chapter Name</th>
<th>Chapter Number</th>
<th>Number Days</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASIA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bahrain</td>
<td>208</td>
<td>12</td>
</tr>
<tr>
<td>Brunei</td>
<td>287</td>
<td>20</td>
</tr>
<tr>
<td>China</td>
<td>46</td>
<td>15</td>
</tr>
<tr>
<td>South Korea</td>
<td>27</td>
<td>20</td>
</tr>
<tr>
<td>India</td>
<td>161</td>
<td>15</td>
</tr>
<tr>
<td>Japan</td>
<td>195</td>
<td>12</td>
</tr>
<tr>
<td>Malaysia</td>
<td>220</td>
<td>15</td>
</tr>
<tr>
<td>Middle East</td>
<td>24</td>
<td>12</td>
</tr>
<tr>
<td>North Asia</td>
<td>112</td>
<td>10</td>
</tr>
<tr>
<td>Pacific</td>
<td>63</td>
<td>12</td>
</tr>
<tr>
<td>Southeast Asia</td>
<td>240</td>
<td>12</td>
</tr>
<tr>
<td>Latin America</td>
<td>23</td>
<td>12</td>
</tr>
<tr>
<td>South America</td>
<td>143</td>
<td>15</td>
</tr>
<tr>
<td>Caribbean</td>
<td>213</td>
<td>12</td>
</tr>
<tr>
<td>Central America</td>
<td>225</td>
<td>15</td>
</tr>
<tr>
<td>South America</td>
<td>126</td>
<td>10</td>
</tr>
<tr>
<td>Mediterranean</td>
<td>61</td>
<td>4</td>
</tr>
<tr>
<td>Iberia</td>
<td>41</td>
<td>12</td>
</tr>
<tr>
<td>Europe/Africa</td>
<td>155</td>
<td>30</td>
</tr>
<tr>
<td>North America</td>
<td>219</td>
<td>15</td>
</tr>
<tr>
<td>Canada</td>
<td>121</td>
<td>30</td>
</tr>
<tr>
<td>United States</td>
<td>225</td>
<td>15</td>
</tr>
<tr>
<td>South America</td>
<td>126</td>
<td>10</td>
</tr>
<tr>
<td>Caribbean</td>
<td>213</td>
<td>12</td>
</tr>
<tr>
<td>Central America</td>
<td>225</td>
<td>15</td>
</tr>
<tr>
<td>South America</td>
<td>126</td>
<td>10</td>
</tr>
</tbody>
</table>

**Note:** Dollar amounts listed below are for local chapter dues. While we expect chapter dues to remain consistent, please check the appropriate chapter dues amount with your remittance.
MEMBERSHIP APPLICATION
Join online and save US $200
www.isaca.org/join

Please complete both sides
U.S. Federal Tax ID No. 48-0732596
Phone: 1-847-660-3505 • Fax: 1-847-285-1443
Email: membership@isaca.org

Name

MIDDLE

LAST NAME

Print name as you want it to appear on membership certificate.

Residence address

Street

CITY STATE/PROVINCE/COUNTRY POSTAL CODE

Residence fax no.

COUNTRY CODE AND NUMBER

Company name

Title

Business address

CITY STATE/PROVINCE/COUNTRY POSTAL CODE

Residence phone

AREA/COUNTRY CODE AND NUMBER

Business phone

AREA/COUNTRY CODE AND NUMBER

E-mail

Send mail to

Home Business

Chapter Affiliation

Chapter Number (please review)

Member’s unique identifier

How did you hear about ISACA?

- ISACA chapter
- ISACA Event
- ISACA Journal
- ISACA Job Fair
- Professional Network
- Do not member
- Publication
- Social Media

Level of education (if applicable for career advancement or personal interest)

- High school
- Bachelor’s degree
- Master’s degree
- PhD
- Six years or more

Certification(s) obtained (other than ISACA, BSISA, EGSP, CISSP, IIPA)

- CPA
- CISSP
- CISM
- CGA
- CGPA
- ISA
- ITIL

Current professional activity

- Director of Technology or IS/IT
- Manager, IS/IT
- IS/IT Consultant
- IS/IT Auditor/Assessor
- IS/IT Staff
- Other

How you heard about ISACA

- ISACA chapter
- ISACA Event
- ISACA Journal
- ISACA Job Fair
- Professional Network
- Do not member
- Publication
- Social Media

Please note: Membership in the association requires you to be in good standing with your professional ethics and conduct. The board of directors may reject any application submitted by ISACA members and nonmembers. If the board determines that the association is not eligible for the price paid, a refund will be issued. If you have any questions about the eligibility of the association, contact ISACA’s membership department by sending your name and address to the attention of Membership Director, ISACA, 600274 + USA

Method of payment

- Check payable to “ISACA” in US dollars, drawn on a bank in the United States.
- Send membership application and payment to the attention of Membership Director, ISACA, 600274 + USA

All payments by credit card will be processed in US dollars

Credit Card 

- American Express
- Diners Club
- MasterCard
- Visa

Firm name of cardholder

Expiration date

Payment due

- Initial membership fee: $135.00 (US)
- Chapter dues (if assessed and paid): $30.00 (US)
- New member processing fee: $50.00 (US)

P. PLEASE PAY THIS TOTAL

$ 195.00

For additional information on ISACA membership, please visit www.isaca.org/ged

Membership dues are non-refundable and non-transferable

Mail your application and check to:

ISACA • 600274 + USA

The deadline amounts on this application are valid 1 August 2019 through 31 May 2020.
<table>
<thead>
<tr>
<th>Chapter Name</th>
<th>Chapter Number</th>
<th>Dues</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASIA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bahrain</td>
<td>228</td>
<td>$25</td>
</tr>
<tr>
<td>China, Hong Kong</td>
<td>227</td>
<td>$20</td>
</tr>
<tr>
<td>India</td>
<td>267</td>
<td>$50</td>
</tr>
<tr>
<td>Indonesia</td>
<td>250</td>
<td>$15</td>
</tr>
<tr>
<td>Iran</td>
<td>164</td>
<td>$50</td>
</tr>
<tr>
<td>Jordan</td>
<td>160</td>
<td>$15</td>
</tr>
<tr>
<td>Japan</td>
<td>160</td>
<td>$50</td>
</tr>
<tr>
<td>Korea</td>
<td>150</td>
<td>$20</td>
</tr>
<tr>
<td>Thailand</td>
<td>140</td>
<td>$30</td>
</tr>
<tr>
<td>Pakistan</td>
<td>140</td>
<td>$50</td>
</tr>
<tr>
<td>Philippines</td>
<td>135</td>
<td>$15</td>
</tr>
<tr>
<td>Malaysia</td>
<td>130</td>
<td>$30</td>
</tr>
<tr>
<td>Vietnam</td>
<td>130</td>
<td>$30</td>
</tr>
<tr>
<td>Singapore</td>
<td>120</td>
<td>$15</td>
</tr>
<tr>
<td>Brunei</td>
<td>120</td>
<td>$20</td>
</tr>
<tr>
<td>Latin America</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Argentina</td>
<td>120</td>
<td>$30</td>
</tr>
<tr>
<td>Bolivia</td>
<td>130</td>
<td>$15</td>
</tr>
<tr>
<td>Brazil</td>
<td>120</td>
<td>$20</td>
</tr>
<tr>
<td>Chile</td>
<td>120</td>
<td>$15</td>
</tr>
<tr>
<td>Colombia</td>
<td>120</td>
<td>$30</td>
</tr>
<tr>
<td>Panama</td>
<td>120</td>
<td>$15</td>
</tr>
<tr>
<td>Paraguay</td>
<td>120</td>
<td>$30</td>
</tr>
<tr>
<td>Peru</td>
<td>120</td>
<td>$30</td>
</tr>
<tr>
<td>Ecuador</td>
<td>120</td>
<td>$30</td>
</tr>
<tr>
<td>Dominican Rep.</td>
<td>120</td>
<td>$30</td>
</tr>
<tr>
<td>Cuba</td>
<td>120</td>
<td>$30</td>
</tr>
<tr>
<td>Mexico</td>
<td>120</td>
<td>$30</td>
</tr>
<tr>
<td>North America</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Canada</td>
<td>120</td>
<td>$30</td>
</tr>
<tr>
<td>United States</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Central US</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Eastern US</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Midwest US</td>
<td></td>
<td></td>
</tr>
<tr>
<td>South US</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Southern US</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Caribbean</td>
<td>130</td>
<td>$30</td>
</tr>
<tr>
<td>Mexico</td>
<td>130</td>
<td>$30</td>
</tr>
<tr>
<td>South America</td>
<td>130</td>
<td>$30</td>
</tr>
<tr>
<td>Europe/Africa</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Austria</td>
<td>150</td>
<td>$40</td>
</tr>
<tr>
<td>Belgium</td>
<td>140</td>
<td>$45</td>
</tr>
<tr>
<td>Bulgaria</td>
<td>130</td>
<td>$50</td>
</tr>
<tr>
<td>Croatia</td>
<td>120</td>
<td>$30</td>
</tr>
<tr>
<td>Cyprus</td>
<td>120</td>
<td>$15</td>
</tr>
<tr>
<td>Czech Republic</td>
<td>130</td>
<td>$150</td>
</tr>
<tr>
<td>Oceania</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Australia</td>
<td>130</td>
<td>$30</td>
</tr>
<tr>
<td>New Zealand</td>
<td>130</td>
<td>$30</td>
</tr>
<tr>
<td>Pacific</td>
<td>130</td>
<td>$30</td>
</tr>
</tbody>
</table>

To receive your copy of the ISAAC Journal, please complete the following subscription information:

- Size of ENTIRE organization
  - Fewer than 50 employees: 50 - 49 employees: 501 - 999 employees: 1000 - 4999 employees: 5000 or more employees:
  - Not applicable

- Size of IT audit staff (full-time equivalent)
  - Individual
  - 2-3 individuals
  - 4-10 individuals
  - 11-24 individuals
  - More than 24 individuals:
  - Not applicable

- Size of information security staff (full-time equivalent)
  - 1 full-time equivalent
  - 2-4 full-time equivalents
  - 5-10 full-time equivalents
  - 11-24 full-time equivalents
  - More than 24 full-time equivalents:
  - Not applicable

Your level of purchasing authority
- Authorized
- Approved

*For current chapter dues, or if the amount is not listed below, please visit the web site, www.isaca.org/chapters, or contact your local chapter at www.isaca.org/chapters.*
# ISACA Student Membership Application

**ISACA**

**www.isaca.org/students**

---

**Name**

- **First**
- **Middle**
- **Last/Family**

**Address at school**

- **City**
- **State/Province/Country**
- **Postal Code**

**Phone at school**

- **Area Code and Number**

**University Name**

- **Expected date of graduation**

**Home Address**

- **City**
- **State/Province/Country**
- **Postal Code**

**Home phone**

- **Area Code and Number**

**E-mail**

---

ISACA requires members to provide certain demographic information to help us understand and better serve our constituents, and to ensure that we deliver information that is relevant to you.

**Send mail to**

- **Home**
- **School**
- **University**

**Degree Program**

- **Undergraduate**
- **Graduate**

**How did you hear about ISACA?**

- **Employee**
- **Referral**
- **Other**

**Verification of Student Status**

To become a student member, you must attach one of the following:

- Current university/college schedule
- Copy of your transcript showing the courses you are taking
- Letter from the College or University stating that you are currently enrolled at the school

**NOTE:** Your printed application form and document verifying your student status are required for processing. Please allow 3-5 business days to obtain your membership number on your membership card or membership card order.

---

**All International Association benefits will be provided electronically.**

---

**Payment due**

- **Membership dues for student**
- **Membership dues for following year**

**PLEASE PAY THIS TOTAL**

---

**Mail your application and check to**

**ISACA • 1055 Pennsylvania Ave. N.W. • Washington, DC 20004• USA**

---

**Method of payment**

- **Check** payable to “ISACA” in US dollars, drawn on US bank
- **Sage**
- **MasterCard** • **Visa**

**All payments by mail must be processed in US dollars**

**Credit Card #**

**Print name of cardholder**

**Expiration date**

**Signature**

---

The dues amount on this application is valid 1 June 2019 through 31 July 2019.
Go Digital
Go Cashless

Say goodbye to the hassles of cash transactions.
Use Canara Bank’s digital banking solutions.

Canara Bank’s Digital Products / Digital Payments Platforms for Cashless Transactions

- BHIM Canara
- BHIM Canara Empower
- BHIM Aadhaar

24 x 7 facility
No wastage of time
Simple to operate
Safe & Secure
Transact from anywhere
No risk of fake currency

Canara PoS Terminals
Can MOBILE
Canara INTERNET BANKING

Debit / Credit Prepaid Cards

*Terms & Conditions apply

Call Canara 1800 425 0018
www.canarabank.com
Your dream home... We make it a reality!

SyndNivas Home Loan
- Buy
- Build
- Renovate

- Affordable rate of interest
- Repayment: up to 30 years or 75 years of age, whichever is earlier
- Hassle-free processing & quick sanction
- Low Processing & documentation charges
- No pre-payment charges

Follow us on:

Toll Free: 1800 3011 3333 | 1800 208 3333

www.syndicatebank.in
Go Digital
Go Cashless

Say goodbye to the
hassles of cash transactions.
Use Canara Bank’s
digital banking solutions.

Canara Bank’s Digital Products /
Digital Payments Platforms for
Cashless Transactions

24 x 7 facility
Transact from anywhere
No wastage of time
Simple to operate
No risk of fake currency
Safe & Secure

Canara
PoS Terminals
Can
MOBILE
Canara
INTERNET BANKING

Call Canara 1800 425 0018
www.canarabank.com
Canara Bank

Go Digital
Go Cashless

Say goodbye to the hassles of cash transactions.
Use Canara Bank’s digital banking solutions.

Canara Bank’s Digital Products /
Digital Payments Platforms for
Cashless Transactions

24 x 7 Facility
No Wastage of time
Simple to operate
No risk of fake currency
Safe & Secure

Call Canara at 1800 425 0018

Your dream home...
We make it a reality!

SyndNivas
Home Loan
Buy • Build • Renovate

- Affordable rate of interest
- Repayment: up to 30 years or 75 years of age, whichever is earlier
- Hassle-free processing & quick sanction
- Low Processing & documentation charges
- No pre-payment charges

Save up to ₹2.67 lakhs as subsidy under PMAY

Follow us on:

www.syndicatebank.in.

Toll Free: 1800 9311 3333 | 1800 208 3333
COBIT Workshop held on 06.07.2019

If undelivered please return to:

ISACA®
Bangalore Chapter

# S.13, 531A, 2nd Floor, Priya Chambers
Dr. Rajkumar Road, 2nd Stage, Rajajinagar
Opp. St. Theresa's Hospital, Bangalore - 560 010.
Ph. : 23377956, Email : chapter@isacabangalore.org

Chapter Reg No : 433/2002-2003